REMARKS

The present application was filed on March 31, 2004 with claims 1 through 27. Claims 1 through 27 are presently pending in the above-identified patent application. Claims 1, 21 and 27 are proposed to be amended.

In the Office Action, the Examiner rejected claim 27 under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter and lacks patentable utility. The Examiner rejected claims 1-27 under 35 U.S.C. §103(a) as being unpatentable over the P-Synch version 6.2 software product, as evidenced by the "P-Synch Installation and Configuration Guide" (hereinafter, "P-Synch"), in view of the web page "SecurityStats.com Password Strength Meter" (hereinafter, SecurityStats.com).

Section 101 Rejection

Claim 27 is rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. As noted by the Examiner, claim 27 is directed to an article of manufacture. As recited in claim 27, as amended, the article of manufacture comprises one or more (novel) programs *on a machine readable recordable medium*. Applicants submit that an article of manufacture is explicitly recognized by section 101 ("manufacture") and is in full compliance with *In re Warmerdam*, 31 USPQ2d 1754, 1759 (Fed. Cir. 1994). Applicants respectfully request withdrawal of the rejection under Section 101.

Independent Claims

Independent claims 1, 21 and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over P-Synch in view of SecurityStats.com.

The Examiner acknowledges that P-Synch does not disclose performing an Internet search using a query containing one or more keywords derived from said proposed password.

The Examiner notes the ability to extend P-Synch to add new rules via a plugin. To be clear, there is no disclosure or suggestion that the plugin allows the step of performing an Internet search using a query containing one or more keywords derived from said proposed password.

The Examiner asserts that SecurityStats.com discloses a web site on the Internet that one can query to determine if a password is sufficiently strong. In addition,

the Examiner notes that SecurityStats.com recommends not using the actual proposed password, but rather something similar.

Each independent claim has been amended to emphasize that the claimed "Internet search" searches *contents of the Internet using a search engine tool.* Support for this amendment can be found in the original specification, for example, at page 9, lines 15-16 ("The analysis correlates the number to the person by analyzing the number of hits obtained by using a search engine (such as Google.com or Orkut.com) where both the person and number appear on the same page.")

SecurityStats.com does not perform an Internet search. Rather, SecurityStats.com allows a user to enter a proposed password to assess the strength of the password. SecurityStats.com explicitly states how the scoring works:

> **How scoring works:** Your password will be checked for complexity against the *guidelines below* (See Suggestions). In addition, your password will also be checked against a *hacking dictionary* containing commonly used passwords and keystroke combinations.

(italics added)

Thus, SecurityStats.com does not disclose or suggest performing and Internet search that searches *contents of the Internet using a search engine tool,* as required by each independent claim, as amended.

Likewise, P-Synch performs a *table look-up* to ensure that one or more rules are not violated. For example, P-Synch ensures that a proposed password is not the user name or a variation thereof.

Applicants submit that P-Synch and SecurityStats.com, alone or in combination, *teach away* from the present invention by suggesting the use of table lookups and dictionary comparisons, respectively.

The present invention, on the other hand, ensures that a proposed password cannot be correlated with the user by performing an *Internet* search using a query containing one or more keywords derived from said proposed password; evaluating results of said search relative to one or more predefined thresholds; and rejecting said

proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results, as required by each independent claim, as amended. See, for example, Published Version of Application, Pars. 40, 65, 74 and 81. In this manner, the present invention is said to ensure that the authentication information provided by a user is not easily obtained through an online search. See, Abstract.

Applicants respectfully request withdrawal of the rejection of the independent claims under Section 103.

Dependent Claims

Claims 2-20 and 22-26 are dependent on independent claims 1 and 21, respectively, and are therefore patentably distinguished over P-Synch and/or Netscape because of their dependency from independent claims 1 and 21 for the reasons set forth above, as well as other elements these claims add in combination to their base claim.

Conclusion

All of the pending claims following entry of the amendments, i.e., claims 1-27, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Respectfully submitted,

/Kevin M. Mason/

Date: April 21, 2008

Kevin M. Mason
Attorney for Applicants
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560